

What is claimed is:

1. A network system providing secure communication service facility, comprising:

central management and control equipment including an  
5 encryption section; and,

a plurality of switching equipment, each including an encryption section;

wherein the encryption section of said central management and control equipment encrypts a public key of switching equipment accommodating a called party, and a common key to  
10 encrypt a message for transmission between switching equipment to perform message communication between a calling party and a called party each time a call requesting secure communication is originated, and the central management and control equipment  
15 delivers the encrypted public key and common key to switching equipment having detected the originated call.

2. The network system according to claim 1,

wherein said central management and control equipment has  
20 a database maintaining public keys of the plurality of switching equipment, and receives from the switching equipment having detected the call a called dial number and a user identification number assigned in said switching equipment,

to retrieve in said database the public key of the switching  
25 equipment accommodating the called dial number, and a public key of the switching equipment detecting the originated call, using the called dial number and the user identification number,

and,

to generate the common key using the retrieved public keys.

3. The network system according to claim 1,

5 wherein said switching equipment having detected the originated call encrypts the common key delivered from the central management and control equipment, using the public key of the switching equipment accommodating the called party, to forward to said switching equipment accommodating the called party,

10 thereby said switching equipment accommodating the called party decrypts the encrypted common key received from the switching equipment having detected the originated call, using a private key maintained in said switching equipment  
15 accommodating the called party.

4. The network system according to claim 1,

wherein said switching equipment detecting the originated call is controlled so as to transit to the secure communication  
20 mode at each time of call origination.

5. The network system according to claim 1,

wherein said switching equipment detecting the originated call is controlled so as to transit to the secure communication  
25 mode by the detection of indication in said call requesting to transit to the secure communication mode.

6. A method for delivering an encryption key to enable secure communication facility provided in a network including central management and control equipment and a plurality of switching equipment, each of said equipment having an encryption section,  
5 the method comprising the steps of:

informing of a called dial number and a user identification number assigned in switching equipment detecting a call from said switching equipment to central management and control equipment;

10 retrieving in a database of the central management and control equipment a public key of switching equipment accommodating a called party using the called dial number; and a public key of the switching equipment detecting the call using the user identification number; to generate a common key using  
15 the retrieved public keys;

encrypting in the switching equipment detecting the call the generated common key using the retrieved public key of the switching equipment accommodating the called party, to forward to said switching equipment accommodating the called party; and,

20 regenerating the common key in the switching equipment accommodating the called party using a private key of said switching equipment accommodating the called party.

7. The method according to claim 6, further comprising the  
25 step of:

encrypting a called dial number and a user identification number assigned in switching equipment detecting the call using

a public key of the central management and control equipment,  
to transfer from said switching equipment detecting the call  
to said central management and control equipment.

SECRET - EOBSE760